CA ERwin® Model Manager

Administration Guide

r7.3

CA Product References

This document references the following CA products:

- CA ERwin® Model Manager (CA ERwin MM)
- CA ERwin® Data Modeler (CA ERwin DM)
- CA ERwin® Process Modeler (CA ERwin PM)
- CA ERwin® Model Navigator (CA ERwin MN)

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, please complete our short customer survey, which is also available on the CA support website, found at http://ca.com/support.

Contents

Chapter 1: Modeling in the Multi-User Environment

CA ERwin MM coordinates the development and management of models created with CA ERwin DM and CA ERwin PM.

This section contains the following topics:

How to Manage Your Licensing

When you purchase a product, you receive a license key. The license key specifies the maximum number of authorized users that your installation supports. Each time you add a user, the number of users is verified to determine if you have exceeded the limits of your license agreement.

As part of the administrative process, you must assign a security profile to each user. When a user enters a login name to connect to the database that houses the CA ERwin MM repository (mart), CA ERwin MM checks whether the login name has a valid security profile and verifies that the maximum number of users is not exceeded. An error message displays when you exceed the maximum number of users permitted by your license.

If you have exceeded your maximum number of users and want to add additional users, you must do *one* of the following:

- Upgrade your license.
- Remove one of the existing users and add the new user.
- Purchase CA ERwin MN, which includes special editions of CA ERwin DM and CA ERwin PM for those users who need read-only access to the mart. You can use CA ERwin MN to open and print models and generate reports, but you cannot save changes to the mart or save to a file. You can use the Security Manager to assign CA ERwin MN users to a special security profile (Guest) that is not counted toward your license agreement.

Enable Windows Authentication

The authentication type determines whether a user connects to the mart using Windows authentication or database authentication. Windows Authentication specifies the use of Windows user names and passwords to secure database access. You must be logged onto your computer as the user who is the dbo of the database. Windows Authentication applies to Oracle Version 9i and 10g or Microsoft SQL Server (2000/2005) users.

To enable Windows authentication

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Drag the icon for the Windows user from the User list onto the security profile icon in the Security Profile list.

   The user is assigned the security profile.

3. Click OK.

   The Windows user name is added to the mart, which enables Windows authentication. The dialog closes.

Important: For Microsoft SQL Server 2000/2005, you must select Mixed Mode Authentication during the installation of the server. For Oracle Version 9i/10g, the following two parameters should be modified in the initialization file (InitSID.ora):

```
Remote_OS_Authent=""
OS_Authent_Prefix=TRUE
```

Microsoft SQL Server 2005 Permissions

For SQL Server 2000, you only need the public permission assigned to save to the mart. However, when the repository is on an SQL Server 2005 instance, you must have the bulkadmin permission designated as well. The ability to do bulk inserts (which was permitted by the public permission, previously) is no longer part of the public permission. As the administrator, you must explicitly define this permission or when you attempt to save a model to a new mart created using a SQL Server 2005 database, an error "You do not have permission to use the bulk load statement." is returned.

Specify Use of Foreign Characters With Microsoft SQL Server 2000

For Microsoft SQL Server 2000, it is necessary to select specific settings in the Client Network Utility to have certain foreign language characters in your models recognized.

To specify the use of foreign characters with Microsoft SQL Server 2000

1. Click Programs, Microsoft SQL Server, Client Network Utility on the Start menu.

   The SQL Server Client Network Utility dialog opens.

2. Select the following check boxes on the DB-Library Options tab:

   - Automatic ANSI to OEM conversion
   - Use international settings

   Click OK.

   Your configuration is set to recognize foreign language characters in your models.

Specify Use of Foreign Characters With Microsoft SQL Server 2005

For Microsoft SQL Server 2005, it is necessary to modify your registry settings to have certain foreign language characters in your models recognized.

To specify the use of foreign characters with Microsoft SQL Server 2005

1. Click Run on the Start menu.

   The Run dialog opens.

2. Enter regedit.

   The Registry Editor opens.

3. Verify or Add the following registry entry:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Client\DB-Lib]

   "AutoAnsiToOem"="ON"

   "UseIntlSettings"="ON"

   Click File, Exit.

   Your configuration is set to recognize foreign language characters in your models.

Custom Security Message at Connection

As the administrator, you can add a custom message on the Connection Manager dialog. The message appears whenever a connection is made to the mart from one of the client applications (CA ERwin DM, CA ERwin PM, or CA ERwin MN). This custom message appears after you are authenticated for connection to the desired mart, but before the connection dialog closes.

A sample stored procedure is provided for each supported database in the Samples folder. It contains enough code to return the message "Welcome to CA ERwin MM". You can modify the sample to change the text or a custom procedure can be written with logic to determine the database user ID and lookup table for an appropriate message to appear. The message can be up to 1000 characters long and the procedure should return 4 separate strings each a maximum of 250 characters in length.

- The following is an example of a stored procedure that can be used on a Microsoft SQL Server or Sybase DBMS to display a custom message at connection:

```
IF EXISTS (SELECT * FROM sysobjects WHERE id = object_id('dbo.m7x_Get_Privacy_Message'))
DROP PROCEDURE dbo.m7x_Get_Privacy_Message
go
CREATE PROCEDURE dbo.m7x_Get_Privacy_Message
  @string1       varchar(250) output,
       @string2       varchar(250) output,
       @string3       varchar(250) output,
       @string4       varchar(250) output
AS
BEGIN
       --Declare
       -- Ensure to initialize strings to avoid un-necessary results
       SELECT    @string1 = '',
                              @string2 = '',
                              @string3 = '',
                              @string4 = ''
   -- Add custom code here for extra validations
  /* Formatted message would go here. Ensure that the content of the message does not exceed 1000 chars. Failure to do so results in truncation */
       Select @string1 = 'This stored procedure will be implemented by the customer based on their current requirements. Depending on the DBMS additional validations can be made by the end user to suit their privacy requirements.'
       Select @string2 = Char(13) + Char(10) + 'Currently the procedure can return up to 1000 characters. Customer responsible for limiting each of the return strings to <= 250 chars, other wise there could be unexpected errors returned by server.'
       Select @string3 = ' Use native DBB functions for special ASCII characters like CRFL, LF, TAB etc.,'
       Select @string4 = Char(13) + Char(10) + 'Prior to exiting the proc make sure to limit the strings to 250 chars'
       -- Safety check to limit 250 chars
```

```
        SELECT   @string1 = left(@string1, 250),
                         @string2 = left(@string2, 250),
                         @string3 = left(@string3, 250),
                         @string4 = left(@string4, 250)
END
go
GRANT ALL ON m7x_Get_Privacy_Message TO PUBLIC
go
```

- The following is an example of a stored procedure that can be used on an Oracle DBMS to display a custom message at connection:

```
CREATE OR REPLACE PROCEDURE m7x_Get_Privacy_Message (
        p$string1   IN OUT varchar2,
        p$string2   IN OUT varchar2,
        p$string3   IN OUT varchar2,
        p$string4   IN OUT varchar2,
   p$gen_err_code IN OUT NUMBER
        )
AS
-- Declarations here
BEGIN
   -- Ensure the return parameter is set to Zero for success
        p$gen_err_code := 0;
        p$string1 := '';
        p$string2 := '';
        p$string3 := '';
        p$string4 := '';
   -- Add custom code here for extra validations
   -- Formatted message would go here. Ensure that the content of the message does not exceed 1000
chars. Failure to do so results in truncation */
        p$string1 := 'This stored procedure will be implemented by the customer based on their current
requirements. Depending on the DBMS additional validations can be made by the end user to suit their
privacy requirements.';
        p$string2 := Chr(13) || Chr(10) || 'Customer responsible for limiting each of the return strings to <= 250
chars, otherwise there could be unexpected errors returned by server.';
        p$string3 := ' Use native DB functions for special ASCII characters like CRFL, LF, TAB etc.,';
        p$string4 := Chr(13) || Chr(10) || 'Prior to exiting the proc make sure to limit the strings to 250 chars';
        -- Safety check to limit 250 chars
        p$string1 := SubStr(p$string1, 1, 250);
        p$string2 := SubStr(p$string2, 1, 250);
        p$string3 := SubStr(p$string3, 1, 250);
        p$string4 := SubStr(p$string4, 1, 250);
        RETURN;
END m7x_Get_Privacy_Message;
/
DROP PUBLIC SYNONYM m7x_Get_Privacy_Message
CREATE PUBLIC SYNONYM m7x_Get_Privacy_Message FOR m7x_Get_Privacy_Message
GRANT ALL ON m7x_Get_Privacy_Message TO PUBLIC
/
```

Add the Stored Procedure to Activate a Custom Message at Connection

As the administrator, you can add a custom message to the Connection dialog based on a stored procedure. If the stored procedure is supplied, then the feature is active, otherwise the feature is dormant. You must create a procedure named M7x_GET_PRIVACY_MESSAGE. During connection to the mart, the existence of the procedure is verified.

To add a stored procedure to activate a custom message at connection

1. Connect to your database editor and copy the sample stored procedure supplied on the product CD in the Samples folder. Make changes to the file and save as a script file.

   The script file is saved.

2. Connect to the mart as the schema owner, and compile the script as M7x_GET_PRIVACY_MESSAGE.

   The procedure is created.

Delete a Mart

As the administrator, you can delete a mart that is no longer active. You must be the database owner (dbo) for Microsoft SQL 2000 Server or Sybase, the database owner (dbo) and have the sysadmin role for Microsoft SQL 2005/2008 Server, or the database schema owner user and the DBA role in Oracle in the target database to create or delete a mart.

Important: Removing the mart is a drastic measure and should only be done after careful consideration. Be sure to back up your database prior to removing the mart in case you want to revert back to the prior version some time in the future. You also must delete the database using your DBMS tools.

To delete a mart

1. Log on to your DBMS machine that contains CA ERwin MM as the dbo or schema owner. Click Programs, CA, ERwin, ERwin Model Manager r7.3, Model Manager on the Start menu.

   The Connection Manager opens.

2. Complete the following information:

   Database

   Identifies the type of relational database management system (DBMS) you will connect to. Select from the current list of supported databases.

   Authentication

   Windows Authentication

   Specifies the use of Windows user names and passwords to secure database access. You must be logged on to your computer as the user who is the dbo of the database. (Available only for Oracle and SQL Server.)

   Database Authentication

   Specifies the use of a local user name and password for the connection.

   Parameters/Value Options

   Connection Type (Microsoft SQL Server 2005 Only)

   Specifies the use of Native Connection to connect using the API provided by the SQL Server Native client software or ODBC data to connect using the ODBC data source you have defined.

   Server

   Identifies the server name.

   Database

   Identifies the name of the CA ERwin MM database or mart.

   Connection String (Oracle Only)

   Specifies the connection string (TNSNames entry).

   You can select a database connection from the Recent Connections panel to automatically populate the Database or Connection String previously used.

   Click Connect.

   The CA ERwin MM Manager opens.

3. Click Delete.

   The mart is deleted.

   Note: Verify that the m7Master and m7License tables no longer exist in the database. If they do exist, remove them manually using your DBMS tools.

Standards Tools

A naming standards tool and data type standards tool help your workgroup create and manage model naming and data type standards. Because naming and data type standards use external files, as the administrator, you can manage these files in CA ERwin MM.

For more information about these tools, see the *CA ERwin DM Online Help*.

Sessions

When you log on to the mart, this event is recorded as the start of a *session*. During a session, the models that you open and the current lock mode of a model are tracked. Each session has its own Action Log, contained in CA ERwin DM, which logs the transaction information containing real-time changes made to a model. After you have logged out of the mart, the Action Log is cleared.

The administrator can terminate a user's session or assign another user the appropriate security permission to terminate user sessions. For example, if a user is working offline on a model and has locked the corresponding model, you can terminate the user's session to unlock the model so that others can access it.

Interrupted Session

If you experience a system failure, all model locks are removed and your session is terminated. When you log back in to the mart, a new session begins. If you proceed, you are notified that the previous connection is terminated.

Terminate a User Session

You can terminate a user's session to prevent the user from saving changes back to the mart. The user is forced to either save their model offline or reconnect to the mart to save their changes. Additionally, you can release the model lock by terminating the user's session.

Note: You must be assigned to the Administrator security profile to terminate a session.

To terminate a session

1. Click Session from the Services menu.

   The Session Manager opens.

2. Select a user in the Users list and click Terminate.

   Any locks that a user placed on models are removed and the selected session is terminated.

Chapter 2: Security

This section contains the following topics:

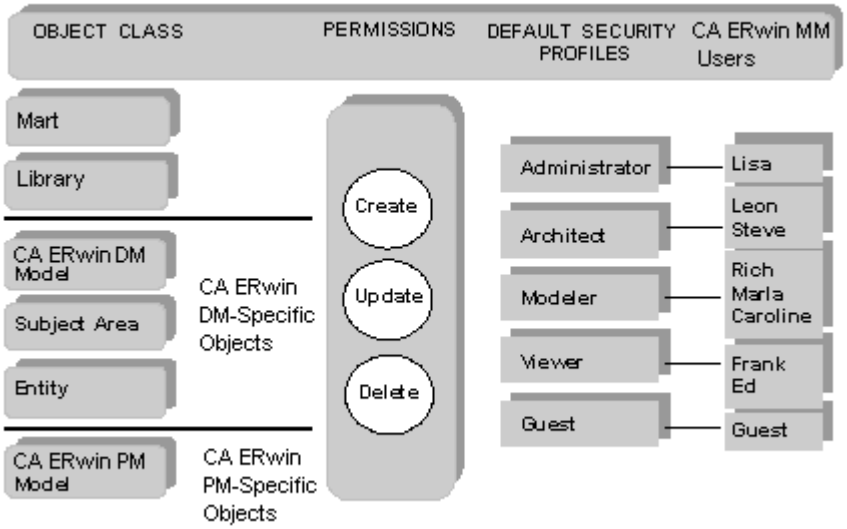
Security

A comprehensive security system prevents unauthorized users from adding, modifying, or deleting objects in the mart. To ensure security, all objects are divided in hierarchical security classes and all users are assigned to a security profile. A security profile is a set of permissions that control the actions a user can perform on a specific group of objects, called a permission object class, in the mart. During installation, five hierarchical security profiles are automatically created. These predefined security profiles are as follows:

- Administrator
- Architect
- Modeler
- Viewer
- Guest

Security profiles determine who can change the data contained in the mart. By understanding the activities that each member of a workgroup performs, you can assign the necessary privileges and customize permissions to meet the exact needs of the workgroup.

When you attempt to create, modify, or delete an object, your security profile determines if the operation is permitted in the mart. Object classes are used to divide objects in hierarchical groups. You can perform an action on an object or be restricted from performing an action on an object based on the security profile. Each profile grants permissions at the object class levels: mart, library, model, subject area, and entity.



Note: Security profiles do not affect the actions you can perform in CA ERwin Data Modeler or CA ERwin Process Modeler. You can create, update, or delete all models locally and you can save your changes to a .erwin file or .bp1 file. However, when you save an updated model back to the mart, you are prohibited from performing any action for which you do not have permission to do.

Inherited Security Permissions

Security permissions for classes that are lower in the hierarchy automatically inherit the security permissions from classes that are higher in the hierarchy, unless specifically overridden by another security profile. For example, if you assign a user the Architect profile for the mart level, the user is automatically assigned Architect-level permissions for all object classes (libraries, diagrams, objects, and properties) below it in the object hierarchy. In this arrangement, you can assign a global security profile to a user at the mart level, and then grant or deny additional permissions in lower-level object classes by assigning a different security profile.

You can also assign a security profile to a user for an individual object. A security profile assigned to a specific object overrides any security permissions inherited from a higher-level object class. If you assign a user to a new security profile, the user retains all permissions granted by other security profiles, except for the permissions that are overridden by the new security profile.

By default, the Viewer and Guest security profiles are read-only security profiles at the mart level. When a user is assigned to a read-only security profile, the permissions defined in that profile are automatically applied to all lower object classes in the database. While you can assign the Viewer profile to limit the permissions of a user in a particular object class, you should use the Guest profile exclusively for users that are using CA ERwin MN to access the database. CA ERwin MM users who are granted a Guest profile do not take up a license. Viewer users do take up a license.

Note: The db_owner of the database always supersedes any security CA ERwin MM provides on the mart. If the db_owner is assigned the Viewer profile, it is still able to change security profiles because the db-owner is the mart administrator by default regardless of the profile assigned in the Security Manager.

Override a User's Inherited Security Permissions

You can override the security permissions automatically inherited by all permission object classes lower in the class hierarchy.

Note: The db_owner of the database always supersedes any security CA ERwin MM provides on the mart. If the db_owner is assigned the Viewer profile, it is still able to change security profiles because the db-owner is the mart administrator by default regardless of the profile assigned in the Security Manager.

To override a user's inherited security permissions

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Click Profile.

   The Security Profile Manager dialog opens.

3. Select the object class or individual object for which you want to override the user's inherited security permissions in the Object list, select or clear the permissions, and click OK.

   The dialog closes and the inherited security permissions are overwritten.

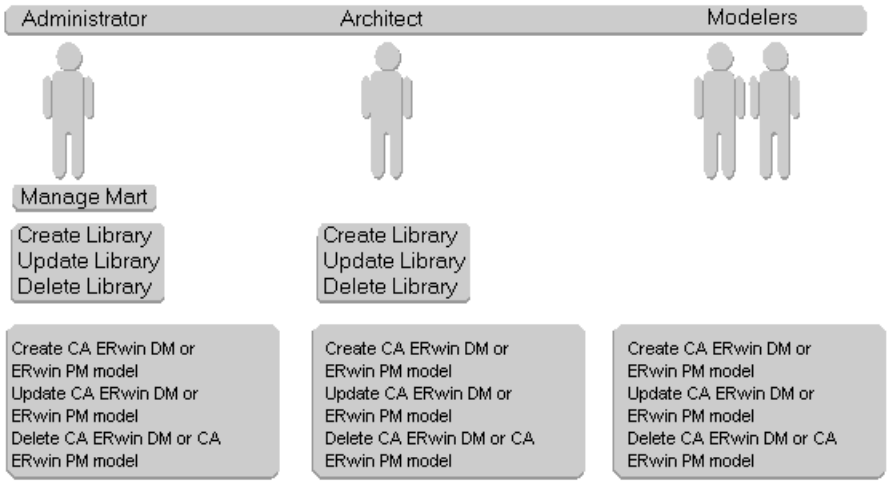
Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Security Management

When you first create the mart, you assign the Administrator security profile to your database user name (the dbo for Microsoft SQL Server or Sybase or the schema owner for Oracle). You can also assign administrator permission to another database user for day-to-day security management.

You can assign users to the predefined security profiles or create customized profiles to fit your environment. You must assign at least one security profile to each user, but you can define an unlimited number of new security profiles and customize the permissions in each profile to manipulate different objects in the mart. For example, you can assign a user to the Architect profile, which grants extensive read or write privileges, in one library and assign the same user to the Viewer profile, which grants no permissions, in a second library.

The following diagram shows the permissions that are granted to the default security profiles:



The role-based security provides complete control over model access and updates, with the flexibility to restrict users by library, model, subject area, and entity. When you assign a security profile to a user, the user is automatically granted equivalent permissions on all lower-level objects unless you specifically assign that user to a different profile for a specific object class.

As the administrator, you can also add and delete users from the mart. Security administration is performed using the Security Manager when connected to CA ERwin MM.

Open the Security Manager

The Security Manager assigns user security profiles and creates custom security profiles. You must be connected to the mart to open the Security Manager. Every user with a security profile is counted as a licensed user. Your registration ID determines the maximum number of users that can access the mart. If the number of users exceeds the limit of your license agreement, a warning message prompts you to remove the unauthorized users.

Note: The Security Manager starts automatically at the end of the installation and initialization process for you to assign user security profiles immediately after you create a mart. You must assign each user to a security profile.

To open the Security Manager, click Security from the Services menu.

The Security Manager opens. You must assign each user to a security profile.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Assign a User to a Security Profile

You can assign a user to a security profile to control the actions that the user can perform on an object. By assigning a user to more than one security profile, you can customize each user's rights to manipulate objects in the mart. You must assign at least one security profile to each user.

Note: The db_owner of the database always supersedes any security CA ERwin MM provides on the mart. If the db_owner is assigned the Viewer profile, it is still able to change security profiles because the db-owner is the mart administrator by default regardless of the profile assigned in the Security Manager.

To assign a user to a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens. The User list contains all the users that have access to the database. When the user is not assigned to any Security Profile, the name icon appears to be grayed out. This means that the user is not able to log-on to the mart.

2. Select the user for which you want to assign security and drag the icon for the user from the User list onto the security profile icon in the Security Profile list.

   The user name displays in the selected security profile. Once the user name is assigned a profile, the icon gets the color to recognize the user name as an active-user.

3. Click OK.

   The dialog closes and the user is assigned to the security profile.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Modify a User's Security Profile

You can assign a user to a particular security profile to control the actions that the user can perform on a given type of object. By assigning a user to more than one security profile, you can customize each user's rights to manipulate objects in the mart. You must assign at least one security profile to each user.

Note: The db_owner of the database always supersedes any security CA ERwin MM provides on the mart. If the db_owner is assigned the Viewer profile, it is still able to change security profiles because the db-owner is the mart administrator by default regardless of the profile assigned in the Security Manager.

To modify a user's security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Expand the list of user names for the appropriate profile in the Security Profile list.

   The user names display in the Security Profile list.

3. Select the user for which you want to modify security permissions and drag the icon for the user from the Security Profile list to the User list.

   The selected user is removed from the Security Profile list.

4. Select the user for which you want to assign security and drag the icon for the user from the User list onto the security profile icon in the Security Profile list.

   The user is assigned the new security profile.

5. Click OK.

   The dialog is closed and the user's security profile is modified.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Assign a Security Profile for a Specific Object

You can assign a security profile for a specific object to control the actions that the user can perform on an object.

Note: The db_owner of the database always supersedes any security CA ERwin MM provides on the mart. If the db_owner is assigned the Viewer profile, it is still able to change security profiles because the db-owner is the mart administrator by default regardless of the profile assigned in the Security Manager.

To assign a security profile for a specific object

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Select the individual object in the Object list for which you want to override the user's inherited security permissions and drag the icon for the user from the User list to a security profile in the Security Profile list.

   The user name displays in the selected security profile. The security profile you assign for a specific object overrides any security permissions inherited from a higher-level permission object class.

3. Click OK.

   The dialog closes and the security profile is assigned for the object.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Remove a User from a Security Profile

You can remove a user from a Security profile, if you no longer want them to have the permissions contained in the security profile.

To remove a user from a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Expand the list of user names for the appropriate profile in the Security Profile list.

   The user names display in the list.

3. Select the user for which you want to remove security permissions and drag the icon for the user from the Security Profile list to the User list.

   The user is removed from the Security Profile list.

4. Click OK.

   The dialog closes and the user is removed from the security profile.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Open the Security Profile Manager

You can change the permissions, modify the default security profiles, or create new security profiles.

Note: The db_owner of the database always supersedes any security CA ERwin MM provides on the mart. If the db_owner is assigned the Viewer profile, it is still able to change security profiles because the db-owner is the mart administrator by default regardless of the profile assigned in the Security Manager.

To open the Security Profile Manager

1. Select Security from the Services menu.

   The Security Manager dialog opens.

2. Click Profile.

   The Security Profile Manager dialog opens.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Add a Security Profile

You can control access to objects and to the tasks users can perform. Security is profile-based and you can add a security profile to restrict access to data in CA ERwin DM by library, model, entity, and subject area; and in CA ERwin PM by library and model.

To add a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Click Profile.

   The Security Profile Manager dialog opens.

3. Click New.

   The Profile Name Editor dialog opens.

4. Enter the name of the new profile in the Name text box, the profile description in the Description text box, and click OK.

   The Profile Name Editor dialog closes.

5. Select the object class in the Object Class list and select or clear the check boxes in the Permission list, and click OK.

   By default, new profiles have no permissions. Permissions are granted or denied for each object class in the new profile. Repeat for each object class to which you want to assign permissions.

   The Security Profile Manager dialog closes.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Modify a Security Profile Name or Description

You can modify a security profile name or description. For instance, if the role of a profile has changed, and you want the name or description of the profile to reflect the new role.

To modify a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Click Profile.

   The Security Profile Manager dialog opens.

3. Select the profile that you want to modify in the Security Profile list and click Edit Profile.

   The Profile Name Editor dialog opens.

4. Modify the profile name or description and click OK.

   The name or description is updated and the Profile Name Editor dialog closes.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Change a Profile's Permissions

You can change the permissions associated with a security profile to restrict access or add access to models.

Note: The db_owner of the database always supersedes any security CA ERwin MM provides on the mart. If the db_owner is assigned the Viewer profile, it is still able to change security profiles because the db-owner is the mart administrator by default regardless of the profile assigned in the Security Manager.

To change the permissions associated with a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Click Profile.

   The Security Profile Manager dialog opens.

3. Select the profile (for example, architect) and click the appropriate object class (for example, mart),

   - To grant permission to perform an activity, select the permission box.
   - To remove permission to perform an activity, clear the permission box.

   Important! Changing the Guest security profile is not permitted.

4. Click OK.

   The permissions are updated for that security profile.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Delete a Security Profile

You can delete a security profile to restrict access to data in CA ERwin DM by library, model, entity, and subject area; and in CA ERwin PM by library and model.

To delete a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Click Profile.

   The Security Profile Manager dialog opens.

3. Select the security profile that you want to delete in the Security Profile list and click Delete.

   The security profile is removed from the list.

4. Click OK.

   The Security Profile Manager closes and the security profile is deleted.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile. While only an administrator can change permissions associated with a profile, anyone can view the permissions.

Chapter 3: Libraries

This section contains the following topics:

Libraries

Libraries are used to store data and business process models that can be shared by users. Libraries can help you organize projects by grouping models together. For example, you can create a library to store models shared by a workgroup, security level, or target server. There is no limit to the number of libraries you can create, and there is no limit to the number of models you can store in a library. By organizing your business process models and data models in libraries, you can also easily manage model merging and conflict resolution.

The administrator must create libraries and determine how to structure the mart for their organization. The administrator can also grant security permission to let other users create, update, or delete a library.

Non-Archiving Libraries

The master model is the master copy of a data model and the most current version stored in the mart. By default, each time you save a model, a version of the model that existed before changes were made is saved. You can enable the creation of models which do not retain multiple versions at the library level from the Library Manager. Libraries which do not retain older model versions are called non-archiving libraries.

For non-archiving libraries, when two or more users modify the same model simultaneously, the original model is not preserved. This is because the Resolve Differences session cannot show if the model changed.

Note: The default setting is to retain multiple model versions in the library.

Library Structure Planning

Before you set up your library structure in the Library Manager, you should review how the workgroup modeling process works in your organization. To help you review your workgroup modeling process, answer the following questions:

- Do you plan to use both CA ERwin DM and CA ERwin PM?
- If using CA ERwin DM and CA ERwin PM with CA ERwin MM, do you plan to share entities and attributes with CA ERwin DM and CA ERwin PM models?
- How will CA ERwin DM models be moved from the development library to the production library?
- How will your approval process for moving models be documented and enforced?
- How will CA ERwin DM models be merged into the enterprise model and who will control this process?
- Will you use versioning to record a model's milestones?
- Who will have what type of access to each library?
- Will CA ERwin DM models be generated to multiple target environments (such as Microsoft SQL Server and Oracle)?
- How will you be warehousing your data?

Library Structure Organization

During the model development life cycle, it is vital that you have an organized library structure so that only those models intended for production are moved to that level. You should structure your libraries in at least three distinct types:

Development Libraries

Contains models that are being created or updated.

Test Libraries

Contains finished models that are being tested prior to moving them to production.

Production Libraries

Contains the finished models that were tested and debugged.

Library Security Levels

After you have created your libraries, determine the security levels for each library. The following three examples should give you an idea of how you can use libraries and security together to help safeguard the project models:

- The entire modeling team can have access to the development library and read-only access to the test and production libraries. Authorized project leaders can be assigned to move models from the development library to the test library, and then from the test to the production library.
- Models from other libraries (for example, Sales and Accounting) can be merged from their own libraries in the enterprise model. Modelers working on projects in the Sales or Accounting libraries can have read-only access to the enterprise library and full access to their own projects. Assign one person or group to manage integration to the enterprise model.
- Modelers need full access to their own libraries and read-only access to the libraries of others. This type of security enhances production because everyone can see what everyone else is working on, all models are stored in one location, and permissions can be changed as different collaborations among modelers become necessary.

Library Structure Considerations

You should consider any or all of these suggestions when building a library structure:

Practical library names

Use practical and functional library names that help all users understand the purpose and type of models contained in the library. For example, you can use the popular format: Short System Name+Version+Stage (for example, Ora_8_Production).

Model naming and datatype standards (CA ERwin DM)

Enforce naming and datatype standards, which is vital to efficient workgroup modeling.

Note: For more information, see the *CA ERwin DM Online Help*.

Rules for model promotion

Define a rigid and documented model approval and promotion process using different libraries for each development phase.

Rules for model versioning

Define versioning rules using different libraries for each development version (for example, Development Beta 1).

User rights and security

Apply stricter rights to libraries that contain mature models nearing the latter stages of development. You can also apply strict rights to individual models.

Publication

Generate reports to communicate milestones in the model development process.

Schema generation rules (CA ERwin DM)

Set up a library where you generate the model schema. Usually, you generate the model schema of promoted models only in the latter stages of development.

Open the Library Manager

You can use the Library Manager to create, rename, and delete libraries, and rename or delete a model. Libraries are managed in the Library Manager in the client product when connected to the mart.

To open the Library Manager, click Library on the Services menu.

The Library Manager opens.

Add a Library

You can add a library to your mart to organize projects by grouping models together for specific purposes or to limit access. For example, you can create separate libraries for data models and process models.

To add a Library

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the mart name in the tree. Enter the new library name in the Name field and click Create.

   Note: The Maintain multiple versions of models in this library check box is selected by default. Clear this check box if you do not want to maintain versioning for this library (non-archiving library).

   The new library is added to the mart.

3. Click Detailed and type a description in the Description box.

   The Details window opens, which shows when the library was created and by whom and any active sessions.

4. Click Brief.

   The Details window closes.

5. Click Close.

   The library is created and the Library Manager dialog closes.

Create a Non-Archiving Library

You can create a new non-archiving library containing models with no versions on them in the mart. All models in the same library either have versioning or not. The default setting is selected which retains multiple versions for models in the library.

To create a non-archiving library

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the mart name at the top of the Directory list and enter a name for the library in the Name text box. Clear the Maintain multiple versions of models in this library check box and click Create.

   The new non-archiving library is created.

Note: For non-archiving libraries, when two or more users modify the same model simultaneously, the original model is not preserved.

Rename a Library

You can rename a library if the name no longer suits the data in the library, for example, a test environment becomes a production environment. You cannot rename a library that has open models.

To rename a library

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the library that you want to rename in the Library list. Enter the new library name in the Name text box and click Update.

   A confirmation dialog opens.

3. Click Yes.

   The library is renamed.

Delete a Library

You can delete a library that is no longer in use, for example a test environment. When you delete a library, all of the models in the mart that belong to that library are also deleted. To preserve a model before you delete the library in which it is stored, you can save the model as a .erwin file or you can save the model in a different library. You cannot delete a library that has open models.

To delete a library

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the library that you want to delete in the Library list and click Delete.

   A confirmation dialog opens.

3. Click Yes.

   The library is deleted.

Update the Library, Model, Version, or Marked Version

You can update the library, model, version, or marked version with description text.

To update the library, model, version, or marked version

1. Click Versions in the Services menu.

   The Version Manager dialog opens.

2. Select library, model, version, or marked version, enter a description in the Description text box and click Update.

   The CA ERwin Data Modeler dialog opens.

3. Click Yes.

   The changes are saved to the library, model, version, or marked version.

Rename a Model from the Library Manager

You can rename a model if the name no longer properly identifies the data. For example, if you want to rename a test model to a production model.

To rename a model

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the model that you want to rename in the Directory list. Enter a new name for the model in the Name text box, and click Update.

   A confirmation dialog opens.

3. Click Yes.

   The model is renamed.

Delete a Model from the Library Manager

You can delete a model that is no longer in use. You cannot delete an open model.

To delete a model

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the model you want to delete in the Directory list and click Delete.

   A confirmation dialog opens.

3. Click Yes.

   The model is deleted.

Chapter 4: Reports

This section contains the following topics:

Workgroup Modeling Reports

Modelers typically work from a common set of libraries, models, and submodels, and must be able to share information about these objects with other users. One way to share information is by using reports, which details the information and definitions for a model in a tabular format.

The Data Browser lets you generate predefined reports to view the contents of specific libraries and models, view the changes and conflicts for specific models, and view the security structure for the database. You can use either the standard or customized reports to see detailed information for a specific model.

All users can run a number of reports in the Data Browser to view the contents of specific libraries and models, and use standard and customized reports to see model information in more detail. However, there are two specific reporting tasks that as the administrator, you can perform:

- Security Manager reports
- Sharing reports

After you generate a report, you can customize the report content and appearance, and then create and save your own custom report views. You can search for information in a report, find a change of value in a column, and hide report rows that do not match the search criteria you specify.

Generate a Security Manager Report

You can generate a report to view information about the security profile assigned to each user and the permissions granted to those profiles. This folder displays in the report tree only when you click Report in the Security Manager dialog.

Note: You must be assigned to the Administrator security profile to run this report.

To generate a Security Manager report

1. Click Security from the Services menu.

   The Security Manager dialog opens.

2. Click Report to open the Data Browser.

   The Data Browser dialog opens.

3. Expand the Security Reports folder and double-click the Security Report you want to run.

   The Security Manager report is generated.

Report Sharing

You can use the Data Browser to select individual reports for company-wide use. The first time you save a report to the mart, a top-level folder called Volume Reports is created. The first time an administrator saves a CA ERwin DM report in CA ERwin Model Manager, the browser creates a new folder called Shared CA ERwin DM Reports.

A user with an Administrator security profile can do the following:

- Copy reports shared in the mart with CA ERwin DM users
- Share CA ERwin DM reports with mart users
- Delete shared reports

If you have the Data Browser open when a change is applied, you do not see the change immediately. You must close and reopen the Data Browser for the change to display.

Important: Version and merging features are not provided for reports. If multiple administrators are editing and saving shared reports to the mart, the changes being made can be inadvertently overwritten. To avoid this problem, you should coordinate editing efforts by multiple administrators.

Share a Mart Report with CA ERwin DM Users

You can copy a shared report from the mart to a local CA ERwin DM folder.

To share a mart report with CA ERwin DM users

1. Log on to the mart that contains the shared report you want to copy, and click Data Browser on the Tools menu.

   The Data Browser opens, and the report names display in the folders.

2. Select the report and select Copy Report to a local file from the Reports menu.

   The selected report is copied to the CA ERwin DM Reports folder.

Share CA ERwin DM Reports with Mart Users

You can copy a CA ERwin DM report to the mart. The browser keeps the folder structure associated with the report and lists it under the Shared CA ERwin DM Reports folder. For example, when the Attributes Report is saved to the mart, it becomes the Shared CA ERwin DM Reports/Attributes Report.

To share CA ERwin DM reports with mart users

1. Log on to the CA ERwin MM mart and click Data Browser on the Tools menu.

   The Data Browser opens.

2. If the report you want to save in CA ERwin MM displays in the active CA ERwin DM Reports (.erp) file, you can copy it to CA ERwin MM by selecting the report in the tree control and choosing the Copy Report to CA ERwin MM option on the Reports menu.

   The report is saved to CA ERwin MM. It can be accessed by other CA ERwin MM users.

Note: If you are having trouble locating the report you want to share, it may not be in the active .erp file. Locate the .erp file containing the report by choosing Open Report File from the Reports menu and specifying the path and file name of the .erp report you want to open.

Delete a Shared Report

You can delete a report in the Volume Reports folder if it no longer needs to be shared.

Note: You must be assigned to the Administrator security profile to delete a report in the Volume Reports folder.

To delete a shared report

1. Log on to the mart in which you want to delete the report, and click Data Browser on the Tools menu.

   The Data Browser opens.

2. Expand the CA ERwin DM Reports folder. Select the report name you want to delete, and click Delete.

   The report is deleted from the Shared CA ERwin DM Reports folder.

Index